

(040830512)

M.Sc. DEGREE EXAMINATION, NOVEMBER 2017

THIRD SEMESTER

Branch – Computer Science

Paper IV — CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours

Max. Marks : 70

SECTION - A

Answer any FIVE questions.

(Marks : 5 × 4 marks = 20 marks)

1. Explain about security services.
2. Discuss about block cipher modes of operations.
3. What are the principles of public key cryptosystems?
4. Explain Euler's theorem.
5. Explain Hash functions.
6. What are the various requirements of authentication?
7. Explain about digital signatures.
8. Explain about firewalls:

SECTION - B

Answer the following questions.

(Marks : 4 × 12.5 marks = 50 marks)

UNIT - I

9. (a) Discuss about steganography.
(b) List out and explain classical encryption techniques.

Or

10. Write a briefly notes on DES algorithm with an encryption and decryptions.

UNIT - II

11. Discuss about confidentiality using conventional encryption.

Or

12. (a) Explain about Diffie – Hellman key exchange algorithm.
(b) Discuss about elliptic curve cryptography.

[P.T.O.]

UNIT - III

13. Explain about message authentication code in detail.

Or

14. Discuss about digital signature standard algorithm in detail.

UNIT - IV

15. What is IP security? Explain IP security architecture.

Or

16. Discuss about E-mail security in detail.
